High-Quality in Data Authentication Dodging Massive Attack in VANETS

Munish Kumar[1], Maninder Kaur, Inderdeep kaur
[1]Research Scholar, DIET Kharar
[2]Assistant Professoer, DIET Kharar
[3]AP(CSE), M.tech Coordintator GGSCMT,Kharar
(E-mail:ggscemunish@gmail.com, manindereceddiet@gmail.com, kaur.inderdeep@gmail.com)

Abstract: -VANET plays an important role in the Security terms. VANET network is due to their unique features like as a high dynamic network (topology) and Mobility prediction. It attracts so much attention to the industry. VANET wireless networks are rapidly increased commercial and academic interests. Mobile connectivity, Traffic congestion management and road safety are some applications that have arisen within this network model. The routing protocol is a reactive type which means if there is data to be sent then the way will create. On-demand Distance Vector routing protocol is a generally used network topology based on rules for VANET. In surveyed of the routing protocol implemented a balance AODV method used for identifying the malicious nodes in the network. A balanced AODV routing method is defined with following characteristics:- (i) Use of threshold adaptive according to the network situations and balance index i.e node nature. (ii) Detect the malicious node in the network. (iii) Detection and prevention methods in real-time and independent on each vehicle node. In research paper, implement a B-AODV routing protocol and RSA method for detection and prevention the malicious node in the vehicular network. In this proposed algorithm, each vehicle node is employing balance index for acceptable and reject able REQ information's (Bits). The consequences of the simulation tool in MATLAB (Matrix Laboratory) indicates BAODV and RSA method is used to detect and prevent the flood attach and loss of network bandwidth. Comparison between AODV, BAODV, RSA in normal phase defines B-AODV is exactly matched with AODV in the vehicular network and performance analysis overhead, an end to end delay and packet delivery rate.

Keywords: *-VANET, Architecture, Routing Protocol, RSA and BAODV protocol.*

*****

I. INTRODUCTION

Major goal of vehicular ad hoc network is to enhance road-safety by utilize of wireless infrastructure. To attain these main goals, vehicular act as a sensor and update each other about ad-normal and potentially dangerous situations like traffic rush, accident and glazes. VANETs closely *gmail.*resemble vehicular ad hoc networks since of their speedily modifying topology [1]. VANETs nearly look like ad-hoc networks need secure routing protocols. Several applications are real to the VEHICULAR setting. In these applications add safety rules applications that would make driver safe, commerce mobile. Road-side services that could intelligently notify drivers in a car about inference, businesses and services in the locality of the vehicular. VEHICULAR AD-HOC NETWORK is normally compared to mobile ad hoc networks are featured by various unique aspects. Vehicular ad hoc networks move with high-velocity, consequence in high-rates of rule modifies. Since of speedily modifying topology due to Vehicular movement, the VANET nearly resembles an ad-hoc network. It constraints and reductions are remarkably dissimilar [2].

From the VANET perspective, security and network scalable are binary important challenges. A set of abuse and hijackers become possible. Hence, the security VANETs are indispensable. The developing significant of inter-vehicular communication has been identified by the GOVT, corporations and the management academic community. Industry and Govt. cooperation has supported large infrastructure vehicular communications partner-ships or projects like as an ADAS (Advanced Driver Assistance Systems) and CARTALK 2000 in Europe, Germany etc. Vehicular ad hoc networks pose several challenges on technology, rules and network security which increase the require for research in the areas [3].

Vehicular ad hoc Network Architecture

Disseminate data in vehicular ad hoc network based on the three architectures [4]:-

(i) Vehicular to Vehicular

V2V environment, where the vehicular act as a every users and producers as a vehicle receive data from the other vehicle node in the network and divided that information to other vehicle nodes in the network. So, every data collection and division of information are completed within the vehicle network for rapid delivery of messages [5].

(ii) Vehicle to Infrastructure

V2I is a wireless architecture, in which environment is utilized to collect data from vehicles and give the data to other vehicle node when required.

(iii) Hybrid Architecture

It is a combination of vehicle to vehicle and vehicle to infrastructure architectures. [6]

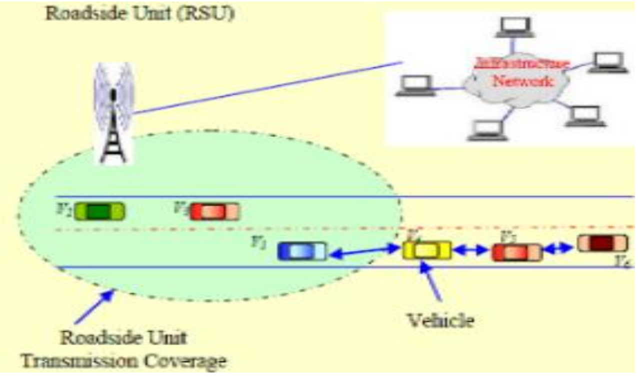

Fig 1 Vehicular ad hoc Network Architecture [17]

Each vehicular node that is a vehicular or road side unit communicates with each other's nodes in single-hop or multi-hop. Vehicular ad hoc networks are developed with the main goals of improving driving safety and giving passenger comfort. In Vehicular ad hoc networks, the various kinds of communication are the following:-

(i) V2V (Vehicle –to- Vehicle)
(ii) Inter-Vehicle
(iii) Communication
(iv) Vehicle- to- Infrastructure
(v) Hybrid Communication

Several Vehicle Ad-Hoc Network the main Challenges are described in below:-

(i) Various hops in data delivery is major challenging task as a frequent disconnection and high-mobility is there in VEHICULAR AD -HOC NETWORK.[7]
(ii) A data connection like as a speed-limit, traffic situations and accident etc. For security and safety and entertainment convenience phases or purposes.
(iii) Vehicle nodes shall be selected for data transferring in, such as a way that data packets would be transmitted in reducing the delay to sink.[8][9]

The main advantages in VANETs:-

(i) Public safety [10]
(ii) Traffic Management
(iii) Traffic co-ordination and Assistance
(iv) Traveller Information Support
(v) Air Pollution emission measurement and reduction.[11]

II. RELATED WORK

Faghihniya, M. J., et al., (2017) [12] proposed a research work on vehicular ad hoc networks which mainly focused to upgrade the security against flooding attack with the use of balance index. VANET stands for vehicular ad hoc networks. Security was the main concern in these kinds of networks. Various approaches and routing protocols were introduced in VANET. A detailed description of vanet, routing protocols was described. AODV was an ad-hoc on demand distance vector which come under the category of reactive protocols. When the data packets were delivered the attackers attack on the layers of network and extract the data. Mostly, in VANET, DDoS attack occurred and it referred to denial of service attack that causes the loss of bandwidth, increased delay and reduced the throughput. To alleviate all these effects of DDoS attack, B-AODV was introduced which was known as balanced ad hoc on demand distance vector. The evaluated outputs depict that it enhanced the network, increment throughput and packet delivery rate.**Sun, C., et al., (2017) [13]** researched on a privacy preserving authentication to decline the denial of service attack in VANET. In this paper a detailed description of authentication, privacy, denial of service attack, classification of routing protocols were given. VANETs were mobile networks that communicate through connections of vehicles and road side units. In this paper a proposed contingent protection saving common verification structure with disavowal of-benefit assault opposition called MADAR. The validation structure consolidates distinctive personality based mark conspires and recognizes inward district and cross-area confirmations to build efficiency. Past the security protection and non-renouncement accomplished by the current system, our validation structure gives awry between vehicle shared verification and quality alterable computational DoS-assault opposition. A formal demonstration about the security protection, un-likability, common credibility, and accuracy of pen name ProVerif, and broke down other security destinations. The execution assessments are led and the outcomes show that our system could accomplish these security destinations with direct calculation and correspondence overheads.**Feng, X., et al., (2017) [14]** deeply described a technique for definesmulti-source Sybil attacks in vehicular ad hoc networks. False messages with different personalities that frequently cause automobile overloads and even prompts vehicular mishaps in vehicular specially appointed system (VANET). It was exceptionally hard to be shielded and distinguished, particularly when it is propelled by some schemed aggressors utilizing their honest to goodness characters. In this paper, an occasion based notoriety framework (EBRS), in which dynamic notoriety and confided in esteem for every occasion are utilized to stifle the spread of false messages. EBRS could distinguish Sybil assault with created characters and stolen personalities during the time spent correspondence, it likewise shields against the contrived Sybil assault since every occasion has exceptional notoriety esteem and confided in esteem.**Waraich P.S., et al., (2017) [15]** explained the preventions against the occurrence of denial of service attack over VANETs with the use of quick response table. Secure directing over VANET is a noteworthy issue due to its high portability condition. Because of dynamic topology, courses were much of the time refreshed and furthermore experiences interface breaks due to the deterrents i.e. structures, passages and extensions and so forth. Visit connect breaks could cause parcel drop and in this manner result in corruption of arrange execution. In the event of VANETs, it turns out to be exceptionally hard to distinguish the reason of the bundle drop as it can likewise happen because of the nearness of a security danger. VANET was a sort of remote ad-hoc arrange and experience the ill effects of regular assaults which exist for portable ad-hoc arrange (MANET) i.e. Disavowal of Services (DoS), Black gap, Gray opening and Sybil assault and so forth. Scientists had officially created different security systems for secure directing over MANET however these arrangements were not completely perfect with special qualities of VANET i.e. vehicles could impart with each other (V2V) and in addition correspondence can be started with foundation based system (V2I). Keeping in mind the end goal to secure the steering for the two kinds of correspondence, there is have to create an answer. In this paper, a technique for secure steering was presented which can distinguish and additionally wipe out the current security danger.**Gillani. S., et al., (2013) [16]** explained the concepts of security in vehicular ad-hoc networks. Vehicular Ad-hoc Networks (VANETs) were the most unmistakable empowering system innovation for Intelligent Transportation Systems. VANETs give numerous new energizing applications and openings but transportation security and assistance applications were in their centre drivers. Security of vehicular systems remains the most huge concerned in VANET organization in light of the fact that it was compulsory to guarantee open furthermore, transportation security. In this paper, the different measurements of VANETs security including security dangers, challenges in giving security in vehicular systems condition, prerequisites and traits of security arrangements. Additionally gives the scientific categorization and basically survey of the eminent security arrangements – accessible for VANETs in writing.

III. PROTOCOLS AND METHODS

These procedures discover the way & maintain it in a table before the sender starts transmitting data. They are further separated into Proactive, Reactive and hybrid procedures.

1.Proactive Protocol

The proactive protocol is also known as table driven routing protocol. These protocols work by periodically exchanging the knowledge of topology between all the knobs of the network. The positive protocols do not have initial route discovery delay but consumes lot of bandwidth for intermittent apprises of topology. There are several routing protocols that fall under this category.[17]

2. Reactive Protocol

These protocols are called as on-demand routing protocols as they periodically update the defeating table, when several data is there to refer. But these protocols use flooding process for route discovery, which reasons more steering overhead & also agonize from the initial route discovery process, which make them unsuitable for safety applications in VANET.[14]

3. Hybrid protocol

HRP is a hybrid protocol that splits the network into numerous zones, which creates a hierarchical protocol as the protocol ZHLS (zone-based hierarchical link state). HRP is based on GPS (Global positioning system), which permits every knob to identify its physical position before mapping an area with table to recognize it to which it fits. The amount of messages exchanged in high ZHLS is what influences the profession of the bandwidth. Our procedure efforts to decrease the number of messages exchanged, thus increasing network performance and service life.[18]

IV. MAIN ISSUES AND CHALLENGES

Privacy preservation is a long-standing issue for VANETs. Various private data, e.g. vehicle's identity, position, moving route, and other driver-specific information, should be protected properly. If these private data are exposed to attackers, they may easily use these data to profile user or launch different attacks, e.g. masquerading attack and impersonation attack. Moreover, a malicious vehicle may send fake messages to misguide other vehicles and cause harm to the road safety. Flooding attack is type of a DoS attack that sources loss of network bandwidth and imposes high overhead to the network. Various approaches have been proposed to support the anonymity of vehicles. One of the most acknowledged mechanisms to ensure the privacy of vehicles for VANET security is privacy-preserving authentication. [19]

Every node in VANETs is equipped with the same wireless communication interface, such as IEEE 802.11p. The nodes are restricted in energy as well as computational and storage competencies. The road side units are anticipated to be trustworthy since they are normally better protected [20]. The related vehicles, on the other hand, are commonly more susceptible to various attacks, and they can be co-operated at any time after the VANET is formed. The adversary can be a stranger located in the wireless range of the vehicles, or the adversary can first cooperation one or more vehicles and behave as an insider later. The adversary is able to eavesdrop, jam, modify, forge, or drop the wireless communication between any devices in range. Flooding attack is type of a denial of facility attack that causes loss of network bandwidth and executes high overhead to the network[21].

IV. RESULT AND DISCUSSIONS

Before we can proceed with performance evaluation, we must choose the different metrics that would help us in making comparisons. There could be different metrics to

determine the performance like throughput, delay, overhead, PDR and Energy. The choice of metric would depend upon the purpose the network has been setup for. The metrics could be related to the different layers of the network stack.
The table below shows different metrics of evaluation, and categories they are appropriate for. Following are some of the performance measurement metrics: -

Table 4.1 Performance Measurement Metrics

Category	**Metric**	**Units**
Buffer Issue	Energy Consumption	Joules (j)
Accuracy	Throughput	%ge
Packets	Packet Delivery Rate	%ge
Routing Issue	Routing Overhead	Db
Routing Issue	Delay	ms

In this section, we discussed the result and discussion in below:-

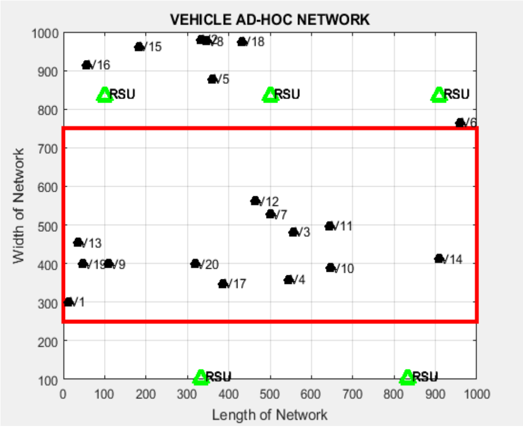

Fig 2. Network Initialization

Above figure shows that the command window, user display the data in command window and Enter the number or vehicle nodes and calculate the area i.e. length and width. It defines that the road side unit plot in the x-axis and y-axis plane. We used the wait base i.e called processed bar to load enter the number of vehicular nodes. It shows that the vehicle nodes plot in the vehicular ad hoc networks.search the source and destination random decide in the vehicular ad hoc networks. The above figure shows the vehicular ad-hoc network architecture and plots the vehicle nodes in the network area and deploys the road side unit. The roadside unit for expanding the availability of vehicular impromptu systems is esteemed essential for adapting to the fractional entrance of Devoted Short Range Correspondences (DSRC) radios into the market at the underlying phases of DSRC sending. After sent the RSU, we found the sound and goal.
In this section, described that the comparative analysis proposed work (B-AODV and RSA) algorithm with existing algorithms (Balance Index).

Table 2:- Comparison between proposed and existing work (Delay)

Algorithms	B-AODV	AODV	B-AODV with RSA
Values in Delay (ms)	1.52	1.63	0.7

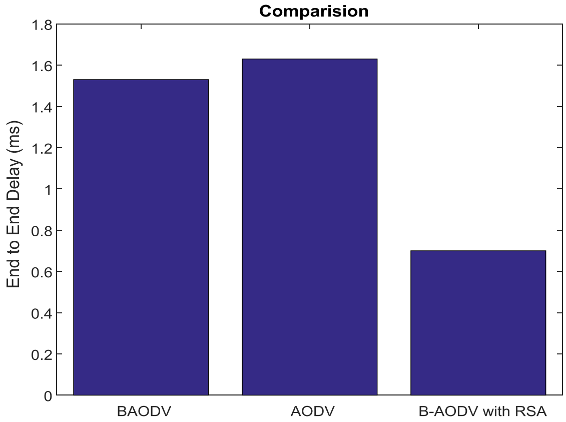

Fig 3. Comparison –Delay (ms)

The above figure 4.17 and Table 4.2 shows that the comparison between proposed (B-AODV with RSA) algorithm and Existing algorithm in (B-AODV and AODV) routing protocols. In proposing algorithm to reduce the delay factor as compared to existing one. The Intruder has come in the VANET network, then request process takes its time.

Table 3:- Comparison between proposed and existing work (PDR)

Algorithms	B-AODV	AODV	B-AODV with RSA
Values in PDR(%)	88	70	89

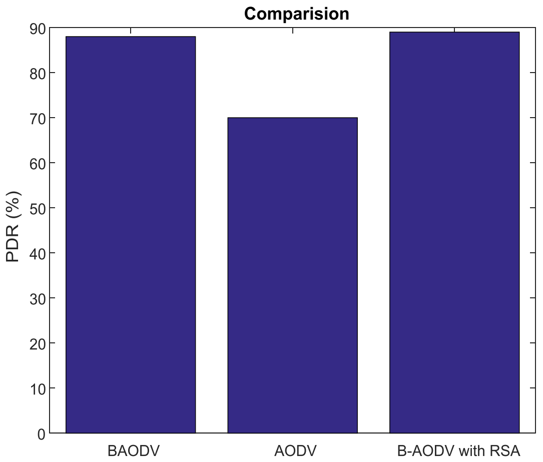

Fig 4Comparison – PDR (%)

Fig 4.and Table 3 the Comparison PDR rate in proposed and existing work enhances the packet delivery rate as compared to the existing routing protocols (B-AODV and AODV). Insecure algorithm has used to improve the delivery rate.

Table 4 :- Comparison between proposed and existing work (Throughput)

Algorithms	B-AODV	AODV	B-AODV with RSA
Values in Throughput (%)	55.4	49.3	89.5

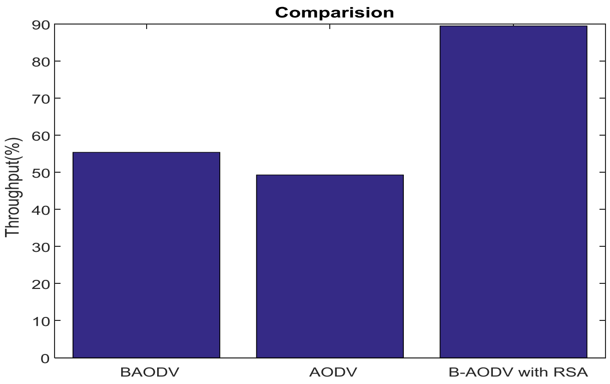

Fig 5.Comparison – Throughput (%)

Fig 5 and Table 4 described that the comparison between proposed algorithm (B-AODV with RSA) and existing protocols (BAODV and AODV) enhances the Throughput as compared to the existing routing protocols (B-AODV and AODV). Insecure algorithm has used to improve the accuracy rate.

V. CONCLUSION AND FUTURE SCOPE

The proposed research work concluded that the routing protocol has been called Balanced ad-hoc network with RSA encryption algorithm. The development of smart vehicle becomes more world-wide spread, the application of network evaluation methodologies to network, in vehicle CSs(Computer Systems) becomes increasingly more vital.

In existing work, the proposed routing protocols for VANETs was implemented and the effect of its parameters on performance like as a delay, throughput, packet delivery and energy consumption for vehicle nodes.

The most vital point of a conclusion from this research work can be explained as follows:-

(i) The proposed routing protocol with encryption algorithm was expected to have good performance compared to real one. As expected, an experiment by the simulation on Network Language (MATLAB 2016a). BAODV with RSA algorithm proved good performance metrics don't have any cons effect like as a PDR (Packet Delivery Rate), E2E delay improvement is very vital in VANET, normally for notification and warning messages.

(ii) Addition to improvement to end to end delay, B-AODV with RSA algorithm can give easy to transmit. This novel improvement is allocated on the application layer.

(iii) The obtaining better consequences in B–AODV and RSA encryption, improvement lead us to enter into the other route to the intended position.

(iv) In this proposed algorithm used in these algorithms to secure the data packets and performance analysis like as a enhance the throughput rate and reduce the delay factor.

Future scope can be extended in dissimilar paths, in the followings some suggested ideas are allowed:-

(i) IDEA algorithm used to enhance the high security (Overload) with and using Hardware sensor to move the vehicle and helps to data transmission in the VANET.

(ii) In IDEA algorithm, will use to encode the information with minimum energy consumed and used the shared key to save the data packets.

REFERENCES

[1]. Ramakrishnan, B., Rajesh, R. S., &Shaji, R. S. (2011). CBVANET: A cluster based vehicular adhoc network model for simple highway communication. *International Journal of Advanced Networking and Applications*, *2*(4), 755-761.

[2]. Maowad, H., &Shaaban, E. (2012, April). Efficient routing protocol for Vehicular Ad hoc networks. In *Networking, Sensing and Control (ICNSC), 2012 9th IEEE International Conference on* (pp. 209-215). IEEE.

[3]. Pathan, A. S. K. (Ed.). (2016). *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press.

[4]. Rawashdeh, Z. Y., & Mahmud, S. M. (2011). Communications in Vehicular Networks. *Mobile Ad-Hoc Networks: Applications, Cap*, *2*, 20-40.

[5]. Kumar, V., & Mishra, S. NarottamChand “Applications of VANETs: Present & Future. *Communications and Networks” in Communications and Networks*, *5*.

[6]. Paul, B., Ibrahim, M., Bikas, M., &Naser, A. (2012). VANET routing protocols: Pros and cons. *arXiv preprint arXiv:1204.1201*.

[7]. Pei, G., Gerla, M., and Chen, T.-W. (2000), “Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks,” Proc. ICC 2000, New Orleans, LA, June 2000.

[8]. Perkins, C.; Belding-Royer, E.; Das, S. (July 2003)”Ad hoc On-Demand Distance Vector (AODV) Routing”.

[9]. Zhao, J.; Cao, G. (2006), "VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks," INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings vol., no., pp.1- 12, April 2006.

[10]. Karp, B. and Kung, H. T (2000), “GPSR: greedy perimeter stateless routing for wireless networks.” In Mobile Computing and Networking, pages 243-254, 2000.

[11]. Lochert, C., Mauve, M., F¨ussler, H., and Hartenstein, H., “Geographic routing in city scenarios,” SIGMOBILE Mob. Comput. Commun. Rev., vol. 9, no. 1, pp. 69–72, 2005.

[12]. Faghihniya, M. J., Hosseini, S. M., &Tahmasebi, M. (2017). Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network. *Wireless Networks*, *23*(6), 1863-1874.

[13]. Sun, C., Liu, J., Xu, X., & Ma, J. (2017). A Privacy-Preserving Mutual Authentication Resisting DoS Attacks in VANETs. *IEEE Access*, *5*, 24012-24022.

[14]. Feng, X., Li, C. Y., Chen, D. X., & Tang, J. (2017). A method for defensing against multi-source Sybil attacks in VANET. *Peer-to-Peer Networking and Applications*, *10*(2), 305-314.

[15]. Waraich, P. S., &Batra, N. (2017, September). Prevention of denial of service attack over vehicle ad hoc networks using quick response table. In Signal Processing, Computing and Control (ISPCC), 2017 4th International Conference on (pp. 586-591). IEEE.

[16]. Gillani, S., Shahzad, F., Qayyum, A., & Mehmood, R. (2013, May). A survey on security in vehicular ad hoc networks. In International Workshop on Communication Technologies for Vehicles (pp. 59-74). Springer, Berlin, Heidelberg.

[17]. Singh, A., & Sharma, P. (2015, December). A novel mechanism for detecting DOS attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA). In Recent Advances in Engineering & Computational Sciences (RAECS), 2015 2nd International Conference on (pp. 1-5). IEEE.

[18]. RoselinMary, S., Maheshwari, M., &Thamaraiselvan, M. (2013, February). Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA). In Information Communication and Embedded Systems (ICICES), 2013 International Conference on (pp. 237-240). IEEE.

[19]. Sharma, P., & Singh, A. (2015). A review on detection and prevention techniques of denial of service attack in vanet. International Journal of Advanced Research in Computer Science, 6(5).

[20]. Kaur, ErGaganpreet, and Sandeep Singh Kang. "Technique to control Data Dissemination and to support data accessibility in Meagerly Connected Vehicles in Vehicular Ad-Hoc Networks (VANETS)." *International Journal of Advanced Research in Computer Science* 7, no. 6 (2016).

[21]. Yang Yang, Qian Liu1, Zhipeng Gao1, Xuesong Qiu1, Lanlan Rui1 and Xin Li, “A data dissemination mechanism for motorway environment in VANETs*”, Springer*, 2015.